REMARKS

This is in response to the non-final Office Action mailed on March 28, 2007. For at least the reasons stated below, Applicants submit the claims are in condition for allowance and patentable over the prior art of record.

Amendments to the Claims

Claims 1, 5 and 8-13 are amended in order to correct certain typographical errors. The amendments to claims 1, 5 and 8-13 do not add any new matter beyond the specification as originally filed. Therefore, Applicants respectfully request entrance and examination.

Rejection of Claims under 35 U.S.C. §101

Claim 1-13 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Specifically, the Examiner asserts that the claimed subject matter does not fall within the statutory classes listed in 35 U.S.C. §101 as the claimed steps do not result in a useful or practical outcome and instead are directed to an abstract idea that fails to produce a real-world result.

Claims 1-13 are currently pending in the present application, with claims 1, 5, 8-13 being Independent claims. Applicants submit that Independent claims 1, 5, 8-13 are directed to a method for determining a network security threat level, with each Independent claim comprising steps to achieve such a determination. Applicants submit that the elements recited in Independent claims 1, 5, 8-13 are, in fact, directed to statutory subject matter.

Specifically, Independent claim 1 contains the claim limitation "calculating a differential threat level by associating the host threat level value with a second host threat level value based upon a second time period wherein the second time period exceeds the first time period." Applicants submit that the claim limitation of "calculating a differential threat level" is a step that provides for the determination of a network security threat level. MPEP § 2106, IV (A) establishes three categories of exceptions to the four statutory categories of invention, (1) abstract ideas, (2) laws of nature and (3) natural phenomena, as non-patentable. The determination of a network security threat level accomplished by "calculating a differential threat level" does not fall within the category of abstract ideas, such as a mathematical algorithm, nor does it fall within the category of the laws of nature or the category of natural phenomena. Instead, "calculating a differential threat level by associating the host threat level value with a second host threat level value based upon a second time period wherein the second time period exceeds the first time period" produces a useful, concrete and tangible result, namely a network security threat level. As the method of Independent claim 1 is not precluded by any of the established categories of non-statutory subject matter under MPEP § 2106, IV and does produce a useful result, Applicants submit that the rejection of Independent claim 1 under 35 U.S.C. §101 should be withdrawn.

Similarly, Independent claim 5 contains the claim limitation, "determining a host threat level based upon a threat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member." Applicants submit that the claim limitation of "determining a host threat level" is a step that provides for the determination of a network security threat level. Likewise, Independent claim 8 contains the claim limitation, "determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member", which is a step that provides for the determination of a network security threat level. In the same way, the claim limitation of Independent Claim 9, "determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination host for the event type", is a step that provides for the determination of a network security threat level. Similarly, Independent claim 10's claim limitation, "calculating the network security threat based upon the source threat, the destination vulnerability, the event validity, and the event severity", is a step that provides for the determination of a network security threat level. Independent claim 11 contains the claim limitation, "calculating a compound host threat by associating a plurality of event threats over a time period with a number of correlated events in the time period", which is a step that provides for the determination of a network security threat level. Independent claim 12's claim limitation, "determining a differential threat level by associating the first compound host threat value with the second host threat value", is a step that provides for the determination of a network security threat level. Finally, Independent claim 13 contains the claim limitation, "calculating a differential threat level by dividing the differential threat level numerator by the differential threat level denominator", which is also a step that provides for the determination of a network security threat level.

As demonstrated above, Independent claims 5 and 8-13 each contain a final claim limitation which provides for the determination of a network security threat level, as in Independent claim 1. Therefore, the final claim limitations identified above for Independent claims 5 and 8-13 demonstrate that the methods of Independent claim 5 and 8-13 produce a useful, concrete and tangible result, namely a network security threat level. Therefore, as Independent claims 5 and 8-13 are not precluded by <u>any</u> of the established categories of non-statutory subject matter under MPEP § 2106, IV and do produce a useful result, Applicants submit that the rejection of Independent claims 5 and 8-13 under 35 U.S.C. §101 should be withdrawn.

Furthermore, dependent claims 2-4 and 6-7 contain additional features and limitations of Independent claims 1 and 5, respectively. Given the Applicants' position on the patentability of the Independent claims 1 and 5, dependent claims 2-4 and 6-7 of the present application are allowable for at least the same reasons as stated above regarding Independent claims 1 and 5.

Therefore, Applicants respectfully traverse and submit that the Examiner misapplies the Examination standard for examining claims under 35 U.S.C. §101 and further request withdrawal of this ground of rejections.

<u>**Rejection of Claims under 35 U.S.C. § 102(e)**</u>

The Examiner rejects pending claims 5-12 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,089,428 B2 to Farley, et al. ("Farley").

Independent claim 5 is directed toward a method for determining network security threat level. The method of claim 5 comprises "receiving event data in response to an identified network event detected by a sensor and based upon the event data, determining a host threat level based upon a threat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member."

The Examiner asserts that the claim element of "determining a host threat level based upon a threat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member" is anticipated by Farley. Specifically, the Examiner points to the fusion engine of Farley which identifies relationships between attacks on hosts identified by intrusion detection systems and generates a correlation event that consists of two sets of lists, inbound attacks relative to the attacked host and outbound attacks relative to the attacked host. (Farley, col. 12, line 30 - col. 13, line 20.) Farley does not disclose using a threat weighting assigned to a host that is associated with a threat weighting assigned to a host network block of which the host is a member in order to determine a threat level. Instead, Farley, at best, describes a process of collecting multiple security threats in order to detect relationships between security threats which may indicate malicious behavior. (Farley, Col. 3, lines 39-43). Farley does not disclose a method which utilizes weighting factors previously assigned in order to determine threat levels. Therefore, the asserted prior art fails to disclose the claim element of "determining a host threat level based upon a threat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member."

Similarly, Independent claims 8 and 10-12 are directed toward a method for determining network security threat level, which comprises the claim element "determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member." The Examiner asserts that the claim element is anticipated by Farley. Similar to the rejection asserted by the

Examiner as to Independent claim 5, the Examiner points to the fusion engine of Farley which identifies relationships between attacks and generates a correlation event that consists of two sets of lists, inbound attacks relative to the attacked host and outbound attacks relative to the attacked host. (Farley, col. 12, line 30 - col. 13, line 20.) As demonstrated above, Farley does not disclose a method that utilizes weighting factors previously assigned in order to determine threat levels, and therefore, fails to disclose the claim element of "determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member."

Similarly, Independent claims 9 and 10-12 are directed towards a method for determining network security threat level, which comprises the claim element "determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member." The Examiner also asserts that the claim element is anticipated by Farley. Specifically, the Examiner points to the use of a Correlation Rule which uses a destination address of an inbound attack to check an attack cache to determine whether there exists other similar attacks. (Farley, col. 19, lines 10-46). As mentioned previously, Farley does not disclose a method which utilizes weighting factors previously assigned in order to determine threat levels. Therefore, the asserted prior art fails to disclose the claim element of "determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member."

Furthermore, dependent claims 6 and 7 contain additional features that further substantially distinguish the invention of the present application over the prior art of record. Given the Applicants' position on the patentability of the Independent claims 5 and 8-12, dependent claims 6 and 7 of the present application are allowable for at least the same reasons as stated above regarding Independent claims 5 and 8 -12.

Rejection of Claims under 35 U.S.C. § 103(a)

The Examiner rejects pending claims 1 and 13 under 35 U.S.C. § 103(a) as being unpatentable over Farley in view of U.S. Patent No 7,152,105 B2 to McClure, et al. ("McClure). The Examiner further rejects pending claims 2-4 under 35 U.S.C. § 103(a) as being unpatentable over Farley in view of McClure and further in view of US Patent No. 6,928,556 B2 to Black, et al. ("Black").

Rejection of Claim 1 under 35 U.S.C. § 103(a)

Independent claim 1 is directed toward a computer-implemented method for determining network security threat level. The method of claim 1 comprises the steps of receiving event data in response to identified network event detected by a sensor and based upon the event data, performing a series of steps. The series of steps includes determining a source threat value, the source threat value based upon a source threat weight for a source IP address and a first range of IP network addresses of which the source IP address is a member. The series of steps further includes determining a destination vulnerability value, the destination vulnerability value based upon the network event in conjunction with a destination IP address, a destination threat weight for the destination IP address, and a threat level value associated with a second range of network IP address of which the destination IP address is a member. Further steps of method 1 include determining an event validity value based upon the source IP address and an event type and determining an event severity value based upon the event type. The remaining steps of the method of claim 1 include calculating an event threat level value based upon the source threat value, the destination vulnerability value, the event validity value, and the event severity value, calculating a host threat level value based upon a summation of event threat level values for a host over a first time period associated with a number of correlated events for the host in the first time period, and calculating a differential threat level by associating the host threat level value with a second host threat level value based upon a second time period wherein the second time period exceeds the first time period.

The Examiner asserts that the claim element of "determining a source threat value, the source threat value based upon a source threat weight for a source IP address and a first range of IP network addresses of which the source IP address is a member" is anticipated by Farley. Similar to the rejection asserted by the Examiner as to Independent claims 5 and 8-12, the Examiner points to the fusion engine of Farley which identifies relationships between attacks and generates a correlation event that consists of two sets of lists, inbound attacks relative to the attacked host and outbound attacks relative to the attacked host. (Farley, col. 12, line 30 - col. 13, line 20.) As demonstrated above, Farley does not disclose a method which utilizes weighting factors previously assigned in order to determine threat levels and therefore, fails to disclose the claim element of "determining a source threat value, the source threat value based upon a source threat weight for a source IP address and a first range of IP network addresses of which the source IP address is a member."

Furthermore, dependent claims 2-4 contain additional features that further substantially distinguish the invention of the present application over the prior art of record. Given the Applicants' position on the patentability of the Independent claim 1, dependent claims 2-4 of the present application are allowable for at least the same reasons as stated above regarding Independent claim 1.

Rejection of Claim 13 under 35 U.S.C. § 103(a)

Independent claim 13 is directed toward a method for determining network security threat level. The method of claim 13 comprises receiving event data in response to an identified network event detected by a sensor, determining an event type based upon the event data and based upon the event data, performing a series of steps. The series of steps includes determining a first host frequency threat level value by summing event threat level values for a host over a first time period dividing by the number of correlated events for the host in the first time period and determining a second host frequency threat level value by summing event threat level values for the host over a second time period greater than the first time period and associated with the number of correlated events for the host in the second time period. Further steps of method 13 include determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period, determining a differential threat level denominator by multiplying the second host frequency value by the first time period, and calculating a differential threat level by dividing the differential threat level numerator by the differential threat level denominator.

The Examiner asserts that the claim elements of "determining a first host frequency threat level value by summing event threat level values for a host over a first time period dividing by the number of correlated events for the host in the first time period", "determining a second host frequency threat level value by summing event threat level values for the host over a second time period greater than the first time period and associated with the number of correlated events for the host in the second time period", "determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period", "determining a differential threat level denominator by multiplying the second host frequency value by the first time period" and "calculating a differential threat level by dividing the differential threat level numerator by the differential threat level denominator" are disclosed by McClure.

In support of the assertion, the Examiner points to preferred embodiments of McClure for a method of assessing the vulnerability of a target computer via a network (McClure, col. 8, line 59 - col. 9, line 40), a method of creating a topographical representation of a network (McClure, col. 9, line 41 - col. 10, line 16) and a method for calculating an objective security score for a network (McClure, col. 10, lines 15 - 28). The method of assessing the vulnerability of a target computer via a network disclosed in McClure does not contain the claim elements of Independent claim 13. At best, McClure's method of assessing the vulnerability of a target computer via a network includes the step of "calculating an objective indicia of security of the network, the calculation based on a weighted summation of confirmed vulnerabilities." (McClure, col.

9, lines 26 - 28). This step does not correlate to "determining a first host frequency threat level value by summing event threat level values for a host over a first time period dividing by the number of correlated events for the host in the first time period", "determining a second host frequency threat level value by summing event threat level values for the host over a second time period greater than the first time period and associated with the number of correlated events for the host in the second time period", "determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period", "determining a differential threat level denominator by multiplying the second host frequency value by the first time period", and finally "calculating a differential threat level by dividing the differential threat level numerator by the differential threat level denominator."

Similarly, the method for calculating an objective security score for a network disclosed in McClure does not contain the elements of Independent claim 13. At best, McClure discloses as a preferred aspect of this method, "the combination of known vulnerabilities is a summation of weighted numeric expressions if particular vulnerabilities, the weighting based on an ease of exploitation ranking and on access ranking for each vulnerability." (McClure, col. 10, lines 23-28). This aspect of the method does not correlate with the claim elements of the method for determining a network security threat level of Independent claim 13. Finally, the method of creating a topographical representation of a network disclosed by McClure does not describe any step remotely similar to the method of claim 13, instead describing the creation and testing of a routing structure.

Applicants respectfully submit that claims 1-13 are allowable in light of the remarks stated above. Therefore, Applicants respectfully request withdrawal of the present rejections and passage of claims to issuance.

For at least all of the above reasons, the Applicants respectfully request that the claims be presented for examination. To expedite prosecution of this application to allowance, the examiner is invited to call the Applicants' undersigned representative to discuss any issues relating to this application.

Dated: August 27, 2007

THIS CORRESPONDENCE IS BEING SUBMITTED ELECTRONICALLY THROUGH THE PATENT AND TRADEMARK OFFICE EFS FILING SYSTEM ON AUGUST 27, 2007.

Respectfully submitted,

Timothy J. Bechen
Reg. No. 48,126
DREIER LLP
499 Park Ave.
New York, New York 10022
Tel : (212) 328-6000
Fax: (212) 328-6001

Customer No. 61834